W2182EM

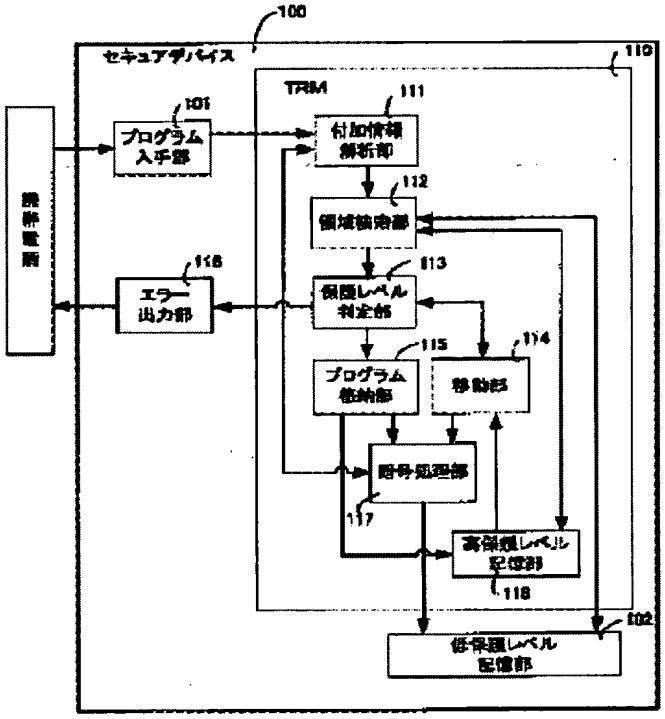
JP2003337749

Patent number: JP2003337749
Publication date: 2003-11-28
Inventor:
Applicant:
Classification:
- international: ***G06F1/00; G06F12/14; G06K19/073; G09C1/00;*** **G06F1/00; G06F12/14; G06K19/073; G09C1/00;** (IPC1-7): G06F12/14; G06F1/00; G06K19/073; G09C1/00
- european:
Application number: JP20030067248 20030312
Priority number(s): JP20030067248 20030312; JP20020068097 20020313

Report a data error here

Abstract of **JP2003337749**

PROBLEM TO BE SOLVED: To provide a secure device capable of downloading a program above a capacity of a storage area mounted inside a TRM while securing safety necessary for a manager of each program. SOLUTION: This secure device 100 storing the program for making it available for use is provided with a low protection level storage part 102, a high protection level storage part 118, a program acquisition part 101 acquiring a program including additional information for specifying a storage destination, an additional information analysis part 111 storing a program matching the additional information in a storage part specified by the acquired additional information, an area retrieval part 112, a protection level determination part 113, and a program storage part 115.
COPYRIGHT: (C)2004,JPO



W2|82EM

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－337749
（P2003－337749A）
(43)公開日　平成15年11月28日(2003.11.28)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード*（参考）
Ｇ０６Ｆ　12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ｋ	５Ｂ０１７
			３１０Ｈ	５Ｂ０３５
1/00		Ｇ０９Ｃ　1/00	６６０Ｄ	５Ｂ０７６
Ｇ０６Ｋ　19/073		Ｇ０６Ｋ　19/00	Ｐ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６６０	Ｇ０６Ｆ　9/06	６６０Ｆ	

審査請求　未請求　請求項の数25　ＯＬ　（全 17 頁）

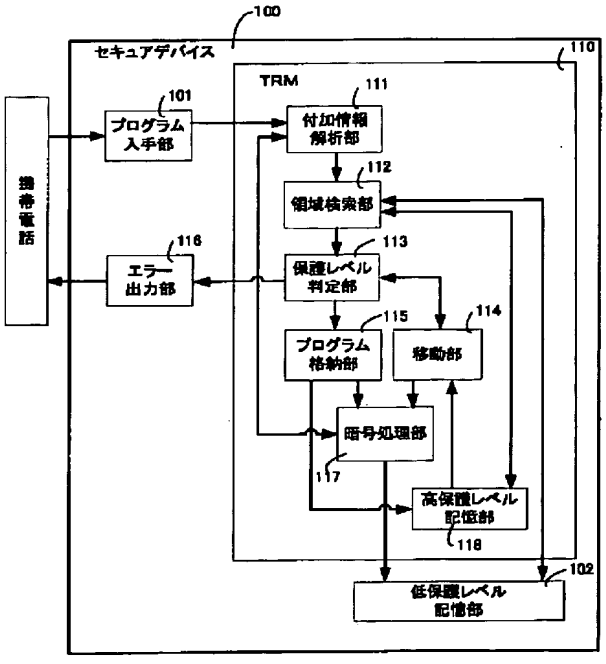
(21)出願番号　特願2003－67248(P2003－67248)
(22)出願日　平成15年３月12日(2003.3.12)
(31)優先権主張番号　特願2002－68097(P2002－68097)
(32)優先日　平成14年３月13日(2002.3.13)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　松崎　なつめ
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　佐久嶋　和生
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100090446
弁理士　中島　司朗

最終頁に続く

(54)【発明の名称】　セキュアデバイス

(57)【要約】
【課題】ＴＲＭ内に実装する記憶領域の容量を越えるプログラムを、各プログラムの管理者が必要とする安全性を確保しつつ、ダウンロードすることができるセキュアデバイスを提供する。
【解決手段】プログラムを格納して利用に供するセキュアデバイス１００であって、低保護レベル記憶部１０２と、高保護レベル記憶部１１８と、格納先を特定するための付加情報を含むプログラムを入手するプログラム入手部１０１と、入手された付加情報により特定される記憶部に当該付加情報に対応するプログラムを格納する付加情報解析部１１１、領域検索部１１２、保護レベル判定部１１３、及びプログラム格納部１１５とを備える。



1

【特許請求の範囲】

【請求項１】　デジタルデータを格納して利用に供するセキュアデバイスであって、

それぞれが記憶領域を備える複数の記憶手段と、

格納先となる記憶手段を特定するための格納先情報が付加されたデジタルデータを入手する入手手段と、

前記格納先情報により特定される記憶手段に、前記デジタルデータを格納する処理手段とを備えることを特徴とするセキュアデバイス。

【請求項２】　前記複数の記憶手段には、それぞれ保護レベルが設定されており、

前記格納先情報は、保護レベルを示し、

前記処理手段は、

前記格納先情報が示す保護レベルと同じ保護レベルが設定されている記憶手段を、前記デジタルデータの格納先として特定することを特徴とする請求項１に記載のセキュアデバイス。

【請求項３】　前記複数の記憶手段には、それぞれ保護レベルが設定されており、

前記格納先情報は、保護レベルを示し、

前記処理手段は、

前記格納先情報が示す保護レベル以上の保護レベルが設定されている記憶手段のうちの１つを、前記デジタルデータの格納先として特定することを特徴とする請求項１に記載のセキュアデバイス。

【請求項４】　前記処理手段は、

前記入手手段により入手された格納先情報が示す保護レベル以上の保護レベルが設定された記憶手段のうち、前記デジタルデータを格納するための空いている記憶領域を確保できる記憶手段を全て検索する検索手段と、

検索手段により検索された記憶手段のうち、一番高い保護レベルが設定されている記憶手段を前記デジタルデータの格納場所として決定する決定手段と、

前記デジタルデータを、決定手段により決定された記憶手段に格納する格納手段とを含むことを特徴とする請求項３に記載のセキュアデバイス。

【請求項５】　前記処理手段は、さらに、

前記検索手段により何れの記憶手段も検索されなかった場合に、利用者にデジタルデータを格納できない旨を提示するためのエラー情報を出力する出力手段を含むことを特徴とする請求項４に記載のセキュアデバイス。

【請求項６】　前記処理手段は、さらに、

前記検索手段により何れの記憶手段も検索されなかった場合に、（１）前記入手手段により入手された格納先情報が示す第１保護レベル以上の保護レベルが設定されている記憶手段に格納されているデジタルデータのそれぞれに付加された格納先情報を読み出し、（２）読み出した格納先情報のうち、それぞれの格納先情報が示す保護レベルが、当該第１保護レベルよりも低い格納先情報を抽出し、（３）抽出した格納先情報に対応するデジタルデータを、当該第１保護レベルよりも低く、且つ、それぞれの格納先情報が示す保護レベル以上の保護レベルが設定されている記憶手段に移動することにより、前記入手手段により入手されたデジタルデータを格納するための記憶領域を確保する移動手段を含み、

前記格納手段は、

移動手段により確保された記憶領域に、前記入手手段により入手されたデジタルデータを格納することを特徴とする請求項４に記載のセキュアデバイス。

【請求項７】　前記移動手段により読み出された格納先情報は、デジタルデータを移動する場合に暗号化するか否かを指定し、

前記移動手段は、

移動すべきデジタルデータに付加された格納先情報に従い、当該デジタルデータを暗号化して移動するか、又は、そのまま移動することを特徴とする請求項６に記載のセキュアデバイス。

【請求項８】　前記移動手段により読み出された格納先情報は、デジタルデータを移動する場合にデジタルデータに改竄検出用の情報を付加するか否かを指定し、

前記移動手段は、

移動すべきデジタルデータに付加された格納先情報に従い、当該デジタルデータに改竄検出用の情報を付加して移動するか、又は、そのまま移動することを特徴とする請求項６に記載のセキュアデバイス。

【請求項９】　前記移動手段により読み出された格納先情報は、デジタルデータを移動する際にデジタルデータにデジタル署名を埋め込むか否かを指定し、

前記移動手段は、

移動すべきデジタルデータに付加された格納先情報に従い、当該デジタルデータにデジタル署名を埋め込んで移動するか、又は、そのまま移動することを特徴とする請求項６に記載のセキュアデバイス。

【請求項１０】　記処理手段は、さらに、

前記移動手段により記憶領域を確保できない場合に、利用者にデジタルデータを格納できない旨を提示するためのエラー情報を出力する出力手段を含むことを特徴とする請求項６に記載のセキュアデバイス。

【請求項１１】　前記複数の記憶手段には、それぞれ保護レベルが設定されており、

前記格納先情報は、保護レベルを示し、さらに、前記対応するデジタルデータの格納先として、当該保護レベルが設定されている記憶手段のみを格納先として特定するか、及び、当該保護レベルが設定されている記憶手段以上の保護レベルが設定された記憶手段を格納先として特定するかのどちらかを指定し、

前記処理手段は、

前記格納先情報に従い、前記格納先情報が示す保護レベルが設定されている記憶手段を、又は、前記格納先情報が示す保護レベル以上の保護レベルが設定されている記

憶手段のうちの１つを、前記デジタルデータの格納先として特定することを特徴とする請求項１に記載のセキュアデバイス。

【請求項１２】　前記格納先情報は、前記対応するデジタルデータの格納先を、当該セキュアデバイスにおいて格納する際に任意に決定してもよいか否かを指定し、

前記処理手段は、

前記格納先情報に従い、任意に決定する記憶手段に、又は、前記格納先情報により特定される記憶手段に、前記デジタルデータを格納することを特徴とする請求項１に記載のセキュアデバイス。

【請求項１３】　前記複数の記憶手段には、それぞれ保護レベルが設定されており、

前記格納先情報は、デジタルデータを所定の保護レベル以下の記憶手段に格納する際に暗号化するか否かを指定し、

前記処理手段は、

デジタルデータを前記所定の保護レベル以下の記憶手段に格納する際に、前記格納先情報に従い、当該デジタルデータを暗号化して格納するか、又は、そのまま格納することを特徴とする請求項１に記載のセキュアデバイス。

【請求項１４】　前記複数の記憶手段には、それぞれ保護レベルが設定されており、

前記格納先情報は、デジタルデータを所定の保護レベル以下の記憶手段に格納する際にデジタルデータに改竄検出用の情報を付加するか否かを指定し、

前記処理手段は、

デジタルデータを前記所定の保護レベル以下の記憶手段に格納する際に、前記格納先情報に従い、当該デジタルデータに改竄検出用の情報を付加して格納するか、又は、そのまま格納することを特徴とする請求項１に記載のセキュアデバイス。

【請求項１５】　前記複数の記憶手段には、それぞれ保護レベルが設定されており、

前記格納先情報は、デジタルデータを所定の保護レベル以下の記憶手段に格納する際にデジタルデータにデジタル署名を埋め込むか否かを指定し、

前記処理手段は、

デジタルデータを前記所定の保護レベル以下の記憶手段に格納する際に、前記格納先情報に従い、当該デジタルデータにデジタル署名を埋め込んで格納するか、又は、そのまま格納することを特徴とする請求項１に記載のセキュアデバイス。

【請求項１６】　前記複数の記憶手段には、それぞれ保護レベルが設定されており、

前記格納先情報は、前記デジタルデータの優先度を示し、

少なくとも１つの記憶手段には、デジタルデータが格納され、

記憶手段に格納されているデジタルデータには、デジタルデータの優先度が設定され、

記憶手段には、より優先度が高いデジタルデータがより保護レベルが高い記憶手段に格納されている状態で、デジタルデータが格納されており、

前記処理手段は、

前記格納先情報により示される優先度に基づいて、前記状態を維持したまま、前記入手手段により入手されたデジタルデータを格納することを特徴とする請求項１に記載のセキュアデバイス。

【請求項１７】　記憶手段に格納されているデジタルデータには、デジタルデータの優先度を示す格納先情報が付加されており、

前記処理手段は、

一番高い保護レベルが設定されている記憶手段から順に、（１）前記入手手段により入手されたデジタルデータを格納するための空いている記憶領域を確保できるか否かを判定し、（２）判定が否定的な場合に、判定対象の記憶手段に格納されているデジタルデータのそれぞれに付加された格納先情報を読み出し、（３）読み出した格納先情報のうち、それぞれの格納先情報が示す優先度が、前記入手手段により入手された格納先情報が示す優先度よりも低い格納先情報を抽出し、（４）抽出した格納先情報を含むデジタルデータを、移動するデジタルデータ対応する保護レベルより低い保護レベルが設定されている記憶手段に移動し、（５）前記判定が肯定的となるまで（１）～（４）の処理を繰り返すことにより、前記入手手段により入手されたデジタルデータを格納するための記憶領域を確保する移動手段と、

移動手段により確保された記憶領域に、前記入手手段により入手されたデジタルデータを格納する格納手段とを含むことを特徴とする請求項１６に記載のセキュアデバイス。

【請求項１８】　前記移動手段により読み出された格納先情報は、デジタルデータを移動する場合に暗号化するか否かを指定し、

前記移動手段は、

移動すべきデジタルデータに付加された格納先情報に従い、当該デジタルデータを暗号化して移動するか、又は、そのまま移動することを特徴とする請求項１７に記載のセキュアデバイス。

【請求項１９】　前記移動手段により読み出された格納先情報は、デジタルデータを移動する場合にデジタルデータに改竄検出用の情報を付加するか否かを指定し、

前記移動手段は、

移動すべきデジタルデータに付加された格納先情報に従い、当該デジタルデータに改竄検出用の情報を付加して移動するか、又は、そのまま移動することを特徴とする請求項１７に記載のセキュアデバイス。

【請求項２０】　前記移動手段により読み出された格納

先情報は、デジタルデータを移動する際にデジタルデータにデジタル署名を埋め込むか否かを指定し、前記移動手段は、
移動すべきデジタルデータに付加された格納先情報に従い、当該デジタルデータにデジタル署名を埋め込んで移動するか、又は、そのまま移動することを特徴とする請求項１７に記載のセキュアデバイス。
【請求項２１】　前記格納先情報は、さらに、保護レベルを示し、
前記移動手段は、
前記入手手段により入手された格納先情報が示す保護レベルより低い保護レベルが設定されている記憶手段においては、前記処理を行わず、
前記処理手段は、さらに、
移動手段により記憶領域を確保できない場合に、利用者にデジタルデータを格納できない旨を提示するためのエラー情報を出力する出力手段を含むことを特徴とする請求項１７に記載のセキュアデバイス。
【請求項２２】　前記入手手段により入手されるデジタルデータはコンピュータプログラムであり、複数のサブプログラムを含み、サブプログラム毎に格納先情報が付加されており、
前記処理手段は、
サブプログラム毎に、それぞれに付加された格納先情報により特定される記憶手段に、対応するサブプログラムを格納することを特徴とする請求項１に記載のセキュアデバイス。
【請求項２３】　前記複数の記憶手段には、それぞれ保護レベルが設定されており、
前記入手手段により入手されるデジタルデータはコンピュータプログラムであり、１つのメインルーチンと複数のサブルーチンを含み、各ルーチン毎に格納先情報が付加され、特にメインルーチンに付加された格納先情報は保護レベルが高い記憶手段に格納すべき事を示し、
前記処理手段は、
ルーチン毎に、それぞれに付加された格納先情報により特定される記憶手段に、対応するルーチンを格納することを特徴とする請求項１に記載のセキュアデバイス。
【請求項２４】　前記入手手段により入手されるデジタルデータには、
当該デジタルデータに付加された格納先情報の正当性を示し、又は、当該デジタルデータと格納先情報の対応が正しいことを示すデジタル署名が埋め込まれているか、又は、認証子が付加されており、
前記処理手段は、
前記デジタル署名、又は、認証子に応じた認証を実施し、当該認証が成功した場合に限り、前記デジタルデータを格納することを特徴とする請求項１に記載のセキュアデバイス。
【請求項２５】　デジタルデータを格納して利用に供するセキュアデバイスにおける格納方法であって、

前記セキュアデバイスは、それぞれが記憶領域を備え、
当該格納方法は、
格納先となる記憶手段を特定するための格納先情報が付加されたデジタルデータを入手する入手ステップと、
前記格納先情報により特定される記憶手段に、前記デジタルデータを格納する処理ステップとを含むことを特徴とする格納方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コンテンツの不正な使用を防止するための技術、及び、電子商取引（モバイルＥＣ）における不正を防止する技術を備えるセキュアデバイスに関する。
【０００２】
【従来の技術】近年、インターネット等のネットワークを介して、音楽コンテンツや動画像コンテンツの配信を受けるコンテンツ配信サービス、及び、モバイルＥＣサービス等の様々な電子情報サービスが普及している。これらの電子情報サービスにおいては、コンテンツの不正な使用を防止するコンテンツ保護技術、及び、モバイルＥＣにおける認証技術や課金技術等のＥＣ保護技術が不可欠であり、これら技術を備えるセキュアデバイスが開発され利用されている。
【０００３】例えば、利用者はこのようなセキュアデバイスを自分の携帯電話に装着して、外出先からコンテンツ配信サービスやモバイルＥＣサービス等を安全に行うことができる。セキュアデバイスについては、「コンテンツ配信・モバイルコマース用のセキュアマルチメディアカード」日立評論２００１年１０月号、三宅順、石原晴次、常広隆司に、コンテンツ保護技術とＥＣ保護技術とを備えるセキュアマルチメディアカード（以下「ＳＭＭＣ」）が記載されている。
【０００４】ＳＭＭＣには、ＪＡＶＡ（登録商標）　Ｃａｒｄのようにプログラムのダウンロード機能を備えるタイプがある。ここでダウンロードされるプログラムは、新規アプリケーションプログラムや、カード内に記録されているプログラムのバージョンアップ版等である。プログラムのダウンロード機能を備えるＳＭＭＣは、ＴＲＭ（ＴａｍｐｅｒＲｅｓｉｓｔａｎｔ　Ｍｏｄｕｌｅ：耐タンパモジュール）内に暗号処理エンジン、セキュリティ鍵情報、ＣＰＵ、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭを備え、また、ＴＲＭ外に大容量のフラッシュメモリ（例えば８ＭＢから２５６ＭＢ程度）を備え、ＣＰＵが暗号処理エンジンやセキュリティ鍵情報を用いて認証処理や暗号処理等を制御し、また、外部よりダウンロードすべきプログラムを取得してＴＲＭ内に実装するＥＥＰＲＯＭに記録して実行する。
【０００５】ここでＴＲＭとは、外部から本モジュール内に記録されているデータの不正な参照や改竄などを困

難にする施策が施されたモジュールである。また、フラッシュメモリには、配信対象である音楽コンテンツや動画像コンテンツ等のデジタルデータが記録される。ＴＲＭ内に実装するＥＥＰＲＯＭは、他のメモリと比較して記憶容量あたりのコストが高く高価なデバイスなので、ＥＥＰＲＯＭの容量を増やすとＳＭＭＣのコストに与える影響が大きい。またデバイスの特性上、ＴＲＭ内に実装するＥＥＰＲＯＭの容量には限界があり、現状ではＥＥＰＲＯＭの容量が６４ＫＢ程度の構成が一般的である。

【０００６】

【非特許文献１】「コンテンツ配信・モバイルコマース用のセキュアマルチメディアカード」日立評論２００１年１０月号、三宅順、石原晴次、常広隆司。

【０００７】

【発明が解決しようとする課題】しかしながら、ＳＭＭＣにダウンロードされるアプリケーションプログラムは今後益々増加するものと予想されるので、現状の構成ではアプリケーションプログラムを、ＴＲＭ内に実装するＥＥＰＲＯＭに格納しきれなくなるのは明らかである。

【０００８】また、ＴＲＭ内に実装するＥＥＰＲＯＭの容量を超えるために記録できないアプリケーションプログラムを、ＴＲＭ外に実装するフラッシュメモリに記録する方法も考えられるが、安全面を考慮すると無秩序にこのような方法を実施することはできず、少なくとも各プログラムの管理者の承認が必要であり、安全性を確保するための新たな技術の確立が望まれる。

【０００９】本発明は、ＴＲＭ内に実装する記憶領域の容量を越えるプログラムを、各プログラムの管理者が必要とする安全性を確保しつつ、ダウンロードすることができるセキュアデバイスを提供することを目的とする。

【００１０】

【課題を解決するための手段】上記目的を達成するために、本発明に係るセキュアデバイスは、デジタルデータを格納して利用に供するセキュアデバイスであって、それぞれが記憶領域を備える複数の記憶手段と、格納先となる記憶手段を特定するための格納先情報が付加されたデジタルデータを入手する入手手段と、前記格納先情報により特定される記憶手段に前記デジタルデータを格納する処理手段とを備えることを特徴とする。

【００１１】上記目的を達成するために、本発明に係る格納方法は、デジタルデータを格納して利用に供するセキュアデバイスにおける格納方法であって、前記セキュアデバイスはそれぞれが記憶領域を備え、当該格納方法は、格納先となる記憶手段を特定するための格納先情報が付加されたデジタルデータを入手する入手ステップと、前記格納先情報により特定される記憶手段に前記デジタルデータを格納する処理ステップとを含むことを特徴とする。

【００１２】これらによって、デジタルデータの管理者がデジタルデータ毎に格納先を設定しておき、ＴＲＭ内に実装するＥＥＰＲＯＭのような保護レベルが高い記憶手段の容量が足らない場合に、各デジタルデータの管理者によって設定された格納先情報に基づいて、管理者によって許可されているデジタルデータであればＴＲＭ外に実装するフラッシュメモリのような保護レベルが低い記憶手段に記録することができるので、デジタルデータを価値に応じて効率よく記録することができる。

【００１３】従って、ＴＲＭ内に実装する記憶領域の容量を越えるプログラムを、プログラムの管理者が必要とする安全性を確保しつつ、ダウンロードすることができる。

【００１４】

【発明の実施の形態】＜概要＞本発明は、保護レベルの異なる複数種類の記憶領域を有するセキュアデバイスが、記憶領域を指定する付加情報を含むデジタルデータを入手して、付加情報に基づいて記憶領域の種類を特定してデジタルデータを記憶するものである。

【００１５】より具体的には、保護レベルが高いＥＥＰＲＯＭと保護レベルが低いフラッシュメモリとの２種類の記憶素子を有するＳＭＭＣにおいて、対応するプログラムを記憶すべき記憶素子がＥＥＰＲＯＭであるかフラッシュメモリであるかを指定する付加情報を含むプログラムを、携帯電話を介してサーバから受信して、付加情報によりＥＥＰＲＯＭ及びフラッシュメモリの何れかを特定し、特定した記憶素子に対応するプログラムをダウンロードするものである。

【００１６】＜システム構成＞図１は、本発明の実施の形態１に係るセキュアシステムの構成を示す図である。図１に示すようにセキュアシステムは、サーバ１、携帯電話２、及び、セキュアデバイス１０から構成される。

【００１７】サーバ１は、予めプログラム毎に付加情報を記録しておき、サーバ１の操作者による指示操作、又は、携帯電話２の利用者による要求操作に応じて、付加情報を含むプログラムを電話回線を介して携帯電話２に送信する。ここで付加情報は、例えばＴＲＭ１２内に実装するＥＥＰＲＯＭ１９であるかＴＲＭ１２外に実装するフラッシュメモリ１８であるかを指定するフラグや、記憶素子毎に設定されている保護レベルを示す数値である。

【００１８】携帯電話２は、電話回線を介してサーバ１から、付加情報を含むプログラムを受信する。セキュアデバイス１０は、例えばＪＡＶＡ（登録商標）　Ｃａｒｄ等のダウンロード機能を備えるＳＭＭＣであり、利用者等によって携帯電話２に装着され、携帯電話２から受信された付加情報を含むプログラムを受取り、付加情報を用いてＥＥＰＲＯＭ１９及びフラッシュメモリ１８の何れかを特定して、特定した記憶素子にプログラムをダウンロードする。

【００１９】セキュアデバイスの外形は、例えば従来の

ＳＭＭＣと同様に切手大程度のサイズや、従来のＩＣカードのサイズであり、他の形状であってもよい。図１に示すようにセキュアデバイス１０は、ＴＲＭ１２外にカードインタフェース回路１１、及び、フラッシュメモリ１８を備え、ＴＲＭ１２内に、暗号処理エンジン１３、セキュリティ鍵情報１４、ＣＰＵ１５、ＲＯＭ１６、ＲＡＭ１７、ＥＥＰＲＯＭ１９、付加情報処理部２０を備える。

【００２０】ここでダウンロードするプログラムは、例えば、有料のアプリケーションプログラム、課金に関わるプログラム、及び、カード内に記録されているプログラムのバージョンアップ版等であり、セキュアデバイス１０において相応の安全性を確保しつつ利用しなければならない。また、ＴＲＭ１２内に実装するＥＥＰＲＯＭ１９は、格納しているプログラムに対して外部から不正なアクセスが出来ず改竄が困難であるので、本明細書において保護レベルが高いと表現する。

【００２１】一方、ＴＲＭ１２外に実装するフラッシュメモリ１８は、格納しているプログラムに対して外部から不正なアクセスが比較的容易にできるので、本明細書において保護レベルが低いと表現する。カードインタフェース回路１１は、携帯電話２とデータのやり取りを行うもであり、携帯電話２から付加情報を含むプログラムを受け取る。

【００２２】ＴＲＭ１２は、耐タンパモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｔ　Ｍｏｄｕｌｅ）であり、内部に記録されているデータに対する外部からの不正なアクセスや改竄を困難にする対策が施された部分である。暗号処理エンジン１３は、プログラムをフラッシュメモリに格納する際に暗号化したり、プログラムの安全性を確認する為に施されたＭＡＣ情報（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）やデジタル署名の認証等を行う。

【００２３】セキュリティ鍵情報１４は、暗号処理エンジン１３による暗号処理や認証処理等に用いられる。付加情報処理部２０は、カードインタフェース回路１１が受け取ったプログラムに含まれる付加情報の意味を解析して、対応するプログラムの格納すべき記憶素子がＥＥＰＲＯＭ１９及びフラッシュメモリ１８の何れであるかを特定する。

【００２４】ＣＰＵ１５は、予めＲＯＭ１６に格納されたプログラムを実行し、ＲＡＭ１７、フラッシュメモリ１８、及び、ＥＥＰＲＯＭ１９を用いて、暗号処理エンジン１３、及び、付加情報処理部２０の制御を行い、付加情報処理部２０により特定された記憶素子に、カードインタフェース回路１１が受け取ったプログラムをダウンロードする。

【００２５】なお、暗号処理エンジン１３、及び、付加情報処理部２０は、ＲＯＭ１６に格納されたプログラムをＣＰＵ１５が実行することにより実現されるものであってもよい。

（実施の形態１）

＜セキュアデバイスの構成＞図２は、本発明の実施の形態１に係るセキュアデバイス１００の構成を示す図である。

【００２６】図２に示すセキュアデバイス１００は、ＴＲＭ１１０外にプログラム入手部１０１、及び、低保護レベル記憶部１０２を備え、ＴＲＭ１１０内に、高保護レベル記憶部１１８、付加情報解析部１１１、領域検索部１１２、保護レベル判定部１１３、移動部１１４、プログラム格納部１１５、エラー出力部１１６、暗号処理部１１７を備える。

【００２７】プログラム入手部１０１は、図１に示したカードインタフェース回路１１に相当し、携帯電話から付加情報を含むプログラムを入手する。低保護レベル記憶部１０２は、例えばＴＲＭ外に実装するフラッシュメモリ等の、保護レベルが低い記憶素子である。高保護レベル記憶部１１８は、例えばＴＲＭ内に実装するＥＥＰＲＯＭ等の、保護レベルが高い記憶素子である。

【００２８】付加情報解析部１１１は、プログラム入手部１０１により入手されたプログラムに含まれる付加情報を解析して、領域検索部１１２、及び、暗号処理部１１７に動作指示を出す。領域検索部１１２は、プログラム入手部１０１により入手されたプログラムを格納できるだけの空いている記憶領域を、付加情報解析部１１１の指示に従って、高保護レベル記憶部１１８、及び、低保護レベル記憶部１０２から検索して、当該記憶領域が存在するか否かを判断する。

【００２９】保護レベル判定部１１３は、領域検索部１１２により検索された記憶領域が、付加情報の意味に適合するかを判定することによって、プログラム入手部１０１により入手されたプログラムの格納場所を決定し、必要に応じてエラー情報を出力するようにエラー出力部１１６に指示する。図３は、本実施の形態１における付加情報を示す図である。

【００３０】図３に示すように本実施の形態１においては、付加情報は５ビットとする。付加情報の下位２ビットは、“００”“０１”“１０”“１１”の４段階の保護レベルのうちの何れかを示す。下位２ビット“００”は、対応するプログラムを高保護レベル記憶部１１８中の空いている記憶領域に格納すべき旨、及び、対応するプログラムを格納できるだけの空いている記憶領域が高保護レベル記憶部１１８中に存在しない場合には格納せずにエラー情報を携帯電話に返すべき旨を意味する。

【００３１】下位２ビット“０１”は、対応するプログラムを高保護レベル記憶部１１８中の空いている記憶領域に格納すべき旨、及び、対応するプログラムを格納できるだけの空いている記憶領域が高保護レベル記憶部１１８中に存在しない場合には、高保護レベル記憶部１１８中の記憶領域を空けて格納する旨を意味する。なお、

下位２ビット“０１”は、他のプログラムが格納されている高保護レベル記憶部１１８中の記憶領域に上書きすべき旨を意味することにしてもよい。

【００３２】下位２ビット“１０”は、対応するプログラムを低保護レベル記憶部１０２に格納すべき旨、及び、対応するプログラムを格納できるだけの空いている記憶領域が低保護レベル記憶部１０２中に存在しない場合には格納せずにエラー情報を携帯電話に返すべき旨を意味する。下位２ビット“１１”は、対応するプログラムを格納できるだけの空いている記憶領域が高保護レベル記憶部１１８中に存在する場合には高保護レベル記憶部１１８に格納すべき旨、存在しない場合には低保護レベル記憶部１０２に格納すべき旨、及び、対応するプログラムを格納できるだけの空いている記憶領域が低保護レベル記憶部１０２中に存在しない場合には格納せずにエラー情報を携帯電話に返すべき旨を意味する。

【００３３】付加情報の下位から３ビット目は、対応するプログラムを低保護レベル記憶部１０２に格納する際に、暗号化するか否かを示す。ここでは下位から３ビット目“０”は、暗号化しない旨を意味し、下位から３ビット目“１”は、暗号化する旨を意味することとする。付加情報の下位から４ビット目は、対応するプログラムを低保護レベル記憶部１０２に格納する際に、ＭＡＣ情報の付加やデジタル署名等を施すか否かを示す。

【００３４】ここでは下位から４ビット目“０”は、ＭＡＣ情報を付加せずデジタル署名を施さない旨を意味し、下位から４ビット目“１”は、ＭＡＣ情報を付加しデジタル署名を施す旨を意味することとする。付加情報の最上位ビット（下位から５ビット目）は、セキュアデバイス１００の利用者が、対応するプログラムの格納場所を自由に決めてよいか否かを示す。

【００３５】ここでは最上位ビット“０”は、格納場所を自由に決めてはならない旨を意味し、最上位ビット“１”は、下位２ビットが示す保護レベルに依存することなく格納場所を自由に決めてよい旨を意味することとする。ここで保護レベル判定部１１３は、高保護レベル記憶部１１８から記憶領域が検索された場合であって、最上位ビットが“０”かつ下位２ビットが“００”、“０１”、“１１”の時には、検索された高保護レベル記憶部１１８中の記憶領域を格納場所に決定する。

【００３６】また保護レベル判定部１１３は、低保護レベル記憶部１０２から記憶領域が検索された場合であって、最上位ビットが“０”かつ下位２ビットが“１０”の時、及び、高保護レベル記憶部１１８から記憶領域が検索されずかつ低保護レベル記憶部１０２から記憶領域が検索された場合であって、最上位ビットが“０”かつ下位２ビットが“１１”の時には、検索された低保護レベル記憶部１０２中の記憶領域を格納場所に決定する。

【００３７】また保護レベル判定部１１３は、高保護レベル記憶部１１８と低保護レベル記憶部１０２との少なくとも一方から記憶領域が検索された場合であって、最上位ビット“１”の時には、検索された何れかの記憶部中の記憶領域を格納場所に決定する。また保護レベル判定部１１３は、高保護レベル記憶部１１８から記憶領域が検索されない場合であって、最上位ビットが“０”かつ下位２ビットが“０１”の時には、移動部１１４に高保護レベル記憶部１１８中の記憶領域を空ける処理を実施するよう指示する。なお、下位２ビット“０１”が、他のプログラムが格納されている高保護レベル記憶部１１８中の記憶領域に上書きすべき旨を意味することにした場合には、他のプログラムが格納されている高保護レベル記憶部１１８中の記憶領域を格納場所に決定する。

【００３８】また保護レベル判定部１１３は、高保護レベル記憶部１１８から記憶領域が検索されない場合であって、最上位ビットが“０”かつ下位２ビットが“００”の時、低保護レベル記憶部１０２から記憶領域が検索されない場合であって、最上位ビットが“０”かつ下位２ビットが“１０”の時、高保護レベル記憶部１１８と低保護レベル記憶部１０２との両方から記憶領域が検索されない場合であって、最上位ビットが“１”の時、又は、最上位ビットが“０”かつ下位２ビットが“１１”の時には、エラー情報を出力するようにエラー出力部１１６に指示する。

【００３９】移動部１１４は、高保護レベル記憶部１１８から記憶領域が検索されず、付加情報の最上位ビット“０”、下位２ビットが“０１”の場合に、高保護レベル記憶部１１８に格納されているプログラムのそれぞれに付加されている付加情報を読み出し、これら付加情報のうち、最上位ビット“０”、又は、下位２ビットが“１１”である付加情報を抽出し、抽出した付加情報に対応するプログラムを低保護レベル記憶部１０２に移動し、プログラム入手部１０１により入手されたプログラムを格納するための記憶領域を高保護レベル記憶部１１８中に確保する。

【００４０】ここで、必要な容量の記憶領域を確保できない場合には、エラー情報を出力するようにエラー出力部１１６に指示する。なお、必要な容量の記憶領域を確保できない場合に、他のプログラムが格納されている高保護レベル記憶部１１８中の記憶領域を格納場所に決定することにしてもよい。プログラム格納部１１５は、保護レベル判定部１１３により決定又は移動部１１４により確保された格納場所に、プログラム入手部１０１により入手されたプログラムを格納する。

【００４１】エラー出力部１１６は、保護レベル判定部１１３によりエラー情報を出力すると決定された場合に、その旨の指示を受けてエラー情報を携帯電話に返し、携帯電話の表示部にデジタルデータを格納できない旨を提示させる。暗号処理部１１７は、セキュアデバイス毎に異なるＩＤ情報を保持し、プログラム入手部１０１により入手されたプログラムを低保護レベル記憶部１

０２に格納する際、及び、プログラムを高保護レベル記憶部１１８から低保護レベル記憶部１０２に移動する際に、付加情報の下位から４ビット目が“１”の場合には、ＭＡＣ情報を付加しデジタル署名を施し、付加情報の下位から３ビット目が“１”の場合には、保持しているＩＤ情報を用いてプログラムを暗号化する。

【００４２】ここで、暗号処理部１１７は、プログラムを高保護レベル記憶部１１８に格納する際にも、付加情報の下位から４ビット目が“１”の場合には、ＭＡＣ情報を付加しデジタル署名を施し、付加情報の下位から３ビット目が“１”の場合には、保持しているＩＤ情報を用いてプログラムを暗号化してもよい。

＜動作＞図４は、本発明の実施の形態１に係るセキュアデバイス１００における、プログラムのダウンロード処理の動作を示す図である。

【００４３】以下に、プログラムのダウンロード処理の動作について説明する。

（１）プログラム入手部１０１が、携帯電話から付加情報を含むプログラムを受け取る（Ｓ１）。

（２）付加情報解析部１１１が、付加情報の最上位ビットが“０”であるか“１”であるかを解析する（Ｓ２）。

【００４４】（３）最上位ビットが“１”である場合は、領域検索部１１２が、プログラム入手部１０１により入手されたプログラムを格納できるだけの空いている記憶領域を、高保護レベル記憶部１１８、及び、低保護レベル記憶部１０２から検索して、当該記憶領域が少なくとも一方の記憶部に存在するか否かを判断する（Ｓ３）。存在しない場合は、エラー処理を行う。

【００４５】（４）存在する場合は、利用者の直接指示や利用者により予め設定されている指示等に基づいて、検索された何れかの記憶部中の記憶領域を格納場所に決定する（Ｓ４）。

（５）最上位ビットが“０”である場合は、保護レベル判定部１１３が、付加情報の下位２ビットが“１０”であるか否かを判定する（Ｓ５）。

【００４６】（６）下位２ビットが“１０”である場合は、領域検索部１１２が、プログラム入手部１０１により入手されたプログラムを格納できるだけの空いている記憶領域が、低保護レベル記憶部１０２に存在するか否かを検索して、当該記憶領域が存在するか否かを判断する（Ｓ６）。存在しない場合は、エラー処理を行う。

（７）存在する場合には、保護レベル判定部１１３が、検索された低保護レベル記憶部１０２中の記憶領域を格納場所に決定する（Ｓ７）。

【００４７】（８）下位２ビットが“１０”でない場合は、領域検索部１１２が、プログラム入手部１０１により入手されたプログラムを格納できるだけの空いている記憶領域が、高保護レベル記憶部１１８に存在するか否かを検索して、当該記憶領域が存在するか否かを判断する（Ｓ８）。

（９）存在する場合には、保護レベル判定部１１３が、検索された高保護レベル記憶部１１８中の記憶領域を格納場所に決定する（Ｓ９）。

【００４８】（１０）存在しない場合には、保護レベル判定部１１３が、付加情報の下位２ビットが“００”であるか否かを判定する（Ｓ１０）。下位２ビットが“００”である場合は、エラー処理を行う。

（１１）下位２ビットが“００”でない場合は、保護レベル判定部１１３が、付加情報の下位２ビットが“０１”であるか否かを判定する（Ｓ１１）。

【００４９】（１２）下位２ビットが“０１”である場合は、移動部１１４が、高保護レベル記憶部１１８に格納されているプログラムを、それぞれに付加されている付加情報に基づいて低保護レベル記憶部１０２に移動し、記憶領域を高保護レベル記憶部１１８中に確保する（Ｓ１２）。確保出来ない場合にはエラー処理を行う。ここで、高保護レベル記憶部１１８に格納されている移動対象のプログラムに、暗号処理部１１７による各処理が施されていない場合には、当該プログラムの移動に際して、付加情報の下位から４ビット目に応じてＭＡＣ情報を付加しデジタル署名を施し、３ビット目に応じてプログラムを暗号化する。

【００５０】（１３）下位２ビットが“０１”でない場合は“１１”であるので、領域検索部１１２が、プログラム入手部１０１により入手されたプログラムを格納できるだけの空いている記憶領域が、低保護レベル記憶部１０２に存在するか否かを検索して、当該記憶領域が存在するか否かを判断する（Ｓ１３）。存在しない場合は、エラー処理を行う。

【００５１】（１４）存在する場合には、保護レベル判定部１１３が、検索された低保護レベル記憶部１０２中の記憶領域を格納場所に決定する（Ｓ１４）。

（１５）プログラム格納部１１５が、決定又は確保された格納場所にプログラムを格納する（Ｓ１９）。ここで、当該プログラムを低保護レベル記憶部１０２に格納する際には、付加情報解析部１１１が付加情報の下位から４ビット目及び３ビット目を解析し、暗号処理部１１７が、解析結果に応じてＭＡＣ情報を付加しデジタル署名を施し、またプログラムを暗号化する。

【００５２】（１６）格納場所を検索又は確保できない場合には、エラー出力部１１６が、エラー情報を携帯電話に返す（Ｓ２０）。

（実施の形態２）

＜セキュアデバイスの構成＞図５は、本発明の実施の形態２に係るセキュアデバイス２００の構成を示す図である。

【００５３】なお、実施の形態１と同様の構成要素には同一番号を付し、その説明を省略する。図５に示すセキュアデバイス２００は、ＴＲＭ２１０外にプログラム入

手部１０１、及び、低保護レベル記憶部１０２を備え、ＴＲＭ２１０内に、高保護レベル記憶部１１８、付加情報解析部１１１、領域検索部１１２、保護レベル判定部２１３、移動部２１４、プログラム格納部１１５、エラー出力部１１６、暗号処理部１１７を備える。

【００５４】保護レベル判定部２１３は、保護レベル判定部２１３は、優先度が高いプログラムから順に高保護レベル記憶部１１８に格納し、高保護レベル記憶部１１８に空き領域が足らなくなったら、低保護レベル記憶部１０２に格納し、必要に応じてエラー情報を出力するようにエラー出力部１１６に指示する。図６は、本実施の形態２における付加情報を示す図である。

【００５５】図６に示すように本実施の形態２においては、付加情報は５ビットとする。付加情報の下位２ビットは、“００”“０１”“１０”“１１”の４段階のプログラムの優先度のうちの何れかを示す。下位２ビット“００”はプログラムの優先度が最も高い事を意味する。下位２ビット“０１”はプログラムの優先度が２番目に高い事を意味する。

【００５６】下位２ビット“１０”はプログラムの優先度が３番目に高い事を意味する。下位２ビット“１１”はプログラムの優先度が４番目に高い事を意味する。付加情報の下位から３ビット目、４ビット目及び最上位ビットは、実施の形態１と同様である。ここで保護レベル判定部２１３は、高保護レベル記憶部１１８から記憶領域が検索された場合には、検索された高保護レベル記憶部１１８中の記憶領域を格納場所に決定する。

【００５７】また保護レベル判定部２１３は、高保護レベル記憶部１１８から記憶領域が検索されなかった場合であって、付加情報の最上位ビット“０”かつ下位２ビットが“００”“０１”“１０”の時には、移動部２１４に高保護レベル記憶部１１８中の記憶領域を空ける処理を実施するよう指示する。また保護レベル判定部２１３は、高保護レベル記憶部１１８から記憶領域が検索されず、低保護レベル記憶部１０２から記憶領域が検索された場合であって、付加情報の最上位ビット“０”かつ下位２ビットが“１１”の時には、検索された低保護レベル記憶部１０２中の記憶領域を格納場所に決定する。

【００５８】移動部２１４は、高保護レベル記憶部１１８から記憶領域が検索されず、付加情報の最上位ビット“０”、下位２ビットが“００”“０１”“１０”の場合に、高保護レベル記憶部１１８に格納されているプログラムのそれぞれに付加されている付加情報を読み出し、これら付加情報のうち、元の付加情報よりも優先度が低い付加情報を抽出し、抽出した付加情報に対応するプログラムを低保護レベル記憶部１０２に移動し、プログラム入手部１０１により入手されたプログラムを格納するための記憶領域を高保護レベル記憶部１１８中に確保する。

【００５９】ここで、記憶領域を高保護レベル記憶部１１８中に確保できなかった場合には、記憶領域を低保護レベル記憶部１０２中に確保する。また、記憶領域を低保護レベル記憶部１０２中にも確保できなかった場合には、保護レベル判定部２１３がエラー情報を出力するようにエラー出力部１１６に指示する。

【００６０】また、例えば、付加情報の下位から２ビット目が“０”の場合には、高保護レベル記憶部１１８にのみ格納を許可するように予め取り決めていたとすると、移動部２１４は下位から２ビット目が“０”の付加情報に対応するプログラムの移動は行わず、また、保護レベル判定部２１３は高保護レベル記憶部１１８中に記憶領域が検索されなかった場合であって、付加情報の下位から２ビット目が“０”の時には、低保護レベル記憶部１０２に記憶領域が検索されたとしても低保護レベル記憶部１０２中の記憶領域を格納場所に決定はせずに、エラー情報を出力するようにエラー出力部１１６に指示する。

【００６１】＜動作＞図７は、本発明の実施の形態２に係るセキュアデバイス２００における、プログラムのダウンロード処理の動作を示す図である。以下に、プログラムのダウンロード処理の動作について説明する。なお、実施の形態１と同様のステップには同一番号を付しその説明を省略する。

【００６２】（１）実施の形態１の（１）と同じ。
（２）実施の形態１の（２）と同じ。
（３）実施の形態１の（３）と同じ。
（４）実施の形態１の（４）と同じ。
（５）最上位ビットが“０”である場合は、領域検索部１１２が、プログラム入手部１０１により入手されたプログラムを格納できるだけの空いている記憶領域が、高保護レベル記憶部１１８に存在するか否かを検索して、当該記憶領域が存在するか否かを判断する（Ｓ２１）。

【００６３】（６）存在する場合には、保護レベル判定部１１３が、検索された高保護レベル記憶部１１８中の記憶領域を格納場所に決定する（Ｓ２２）。
（７）存在しない場合には、保護レベル判定部１１３が、付加情報の下位２ビットが“１１”であるか否かを判定する（Ｓ２３）。
（８）下位２ビットが“１１”である場合は、領域検索部１１２が、プログラム入手部１０１により入手されたプログラムを格納できるだけの空いている記憶領域が、低保護レベル記憶部１０２に存在するか否かを検索して、当該記憶領域が存在するか否かを判断する（Ｓ２４）。存在しない場合は、エラー処理を行う。

【００６４】（９）存在する場合には、保護レベル判定部１１３が、検索された低保護レベル記憶部１０２中の記憶領域を格納場所に決定する（Ｓ２５）。
（１０）下位２ビットが“１１”でない場合は、移動部２１４が、高保護レベル記憶部１１８に格納されているプログラムのそれぞれに付加されている付加情報を読み

出し、これら付加情報のうち、元の付加情報よりも優先度が低い付加情報を抽出し、抽出した付加情報に対応するプログラムを低保護レベル記憶部１０２に移動し、プログラム入手部１０１により入手されたプログラムを格納するための記憶領域を高保護レベル記憶部１１８中に確保する（Ｓ２６）。

【００６５】ここで、高保護レベル記憶部１１８に格納されている移動対象のプログラムに、暗号処理部１１７による各処理が施されていない場合には、当該プログラムの移動に際して、付加情報の下位から４ビット目に応じてＭＡＣ情報を付加しデジタル署名を施し、３ビット目に応じてプログラムを暗号化する。

（１１）記憶領域を高保護レベル記憶部１１８中に確保できない場合には、記憶領域を低保護レベル記憶部１０２中に確保する（Ｓ２７）。記憶領域を低保護レベル記憶部１０２中にも確保できない場合には、エラー処理を行う。

【００６６】（１２）実施の形態１の（１５）と同じ（Ｓ１５）。

（１３）実施の形態１の（１６）と同じ（Ｓ１６）。

（変形例）なお、付加情報は対応するプログラムと切り離しができないように、プログラムファイルのヘッダに付加情報をプログラムＩＤと共に記録し、ヘッダを含むプログラムファイル全体に対して、ＭＡＣ情報を付加したりデジタル署名を施し、本発明のセキュアデバイスがプログラムのダウンロードの条件として、ＭＡＣ情報やデジタル署名の認証を行なってもよいし、また、プログラムを実行することにより付加情報を出力するものであってもよい。

【００６７】また、本発明の実施の形態１及び２では、付加情報をプログラムと共に格納し、格納したプログラムを移動する際に用いているが、移動等を行なわず格納後に付加情報を使わない場合には付加情報を格納しなくてもよいので、付加情報を除いてプログラムのみを格納しても構わない。また、本発明の実施の形態１及び２では、プログラムを格納する記憶素子として、保護レベルが異なる２種類の記憶素子を用いて説明したが、保護レベルが異なる３種類以上の記憶素子を用いても同様に実施できる。

【００６８】また、本発明の実施の形態１及び２では、プログラム毎に付加情報を対応付けているが、１つのプログラムに複数の付加情報を対応付けてもよい。例えば、１つのプログラムを複数のサブプログラムに分割してサブプログラム毎に付加情報を対応付けることによって、決算プログラムの中で料金を直接処理しているような秘匿性の高いサブプログラムだけを保護レベルの高い記憶素子に格納することができる。また例えば、プログラム中のメインルーチンと各サブルーチンを分離して各ルーチン毎に付加情報を対応付け、メインルーチンを保護レベルの高い記憶素子に格納することによってプログラムを難読化することができ、あるいは、各サブルーチンのうち秘匿性の高いサブルーチンだけを保護レベルの高い記憶素子に格納することができる。

【００６９】また、本発明の実施の形態１及び２では、ダウンロードの対象をプログラムとして説明したが、デジタルコンテンツであってもよいし、他のデジタルデータであってもよい。

（まとめ）以上のように、本発明のセキュアデバイスによれば、プログラムに含まれる付加情報に基づいてプログラムの格納場所を決定する事ができるので、プログラムの管理者が付加情報を予め設定しておくことによって、ＴＲＭ内に実装する記憶領域の容量を越えるプログラムを、各プログラムの管理者が必要とする安全性を確保しつつ、ダウンロードすることができる。

【００７０】ここで、産業上の利用の可能性という観点で考えると、本発明は、インターネット等のネットワークを介して、音楽コンテンツや動画像コンテンツの配信を受けるコンテンツ配信サービス、及び、モバイルＥＣサービス等の様々な電子情報サービスに適用することができる。本発明のセキュアデバイスにより、ＴＲＭ内に実装する記憶領域の容量を越えるプログラムを、各プログラムの管理者が必要とする安全性を確保しつつダウンロードすることができ、利用者は本発明のセキュアデバイスを自分の携帯電話に装着して、外出先からコンテンツ配信サービスやモバイルＥＣサービス等を安全に行うことができる。

【００７１】

【発明の効果】本発明に係るセキュアデバイスは、デジタルデータを格納して利用に供するセキュアデバイスであって、それぞれが記憶領域を備える複数の記憶手段と、格納先となる記憶手段を特定するための格納先情報が付加されたデジタルデータを入手する入手手段と、前記格納先情報により特定される記憶手段に前記デジタルデータを格納する処理手段とを備えることを特徴とする。

【００７２】本発明に係る格納方法は、デジタルデータを格納して利用に供するセキュアデバイスにおける格納方法であって、前記セキュアデバイスはそれぞれが記憶領域を備え、当該格納方法は、格納先となる記憶手段を特定するための格納先情報が付加されたデジタルデータを入手する入手ステップと、前記格納先情報により特定される記憶手段に前記デジタルデータを格納する処理ステップとを含むことを特徴とする。

【００７３】これらによって、デジタルデータの管理者がデジタルデータ毎に格納先を設定しておき、ＴＲＭ内に実装するＥＥＰＲＯＭのような保護レベルが高い記憶手段の容量が足らない場合に、各デジタルデータの管理者によって設定された格納先情報に基づいて、管理者によって許可されているデジタルデータであればＴＲＭ外に実装するフラッシュメモリのような保護レベルが低い

記憶手段に記録することができるので、デジタルデータを価値に応じて効率よく記録することができる。

【００７４】従って、ＴＲＭ内に実装する記憶領域の容量を越えるプログラムを、プログラムの管理者が必要とする安全性を確保しつつ、ダウンロードすることができる。また、セキュアデバイスにおいて、前記複数の記憶手段にはそれぞれ保護レベルが設定されており、前記格納先情報は保護レベルを示し、前記処理手段は、前記格納先情報が示す保護レベルと同じ保護レベルが設定されている記憶手段を前記デジタルデータの格納先として特定することを特徴とすることもできる。

【００７５】これによって、デジタルデータの管理者がデジタルデータ毎に保護レベルを設定しておき、保護レベルが一致する記憶手段を格納先として特定することができるので、デジタルデータを価値に応じて効率よく記録することができる。また、セキュアデバイスにおいて、前記複数の記憶手段にはそれぞれ保護レベルが設定されており、前記格納先情報は保護レベルを示し、前記処理手段は、前記格納先情報が示す保護レベル以上の保護レベルが設定されている記憶手段のうちの１つを前記デジタルデータの格納先として特定することを特徴　とすることもできる。

【００７６】これによって、デジタルデータの管理者がデジタルデータ毎に保護レベルを設定しておき、保護レベルが同等以上の記憶手段を格納先として特定することができるので、デジタルデータを価値に応じて効率よく記録することができる。また、セキュアデバイスにおいて、前記処理手段は、前記入手手段により入手された格納先情報が示す保護レベル以上の保護レベルが設定された記憶手段のうち前記デジタルデータを格納するための空いている記憶領域を確保できる記憶手段を全て検索する検索手段と、検索手段により検索された記憶手段のうち一番高い保護レベルが設定されている記憶手段を前記デジタルデータの格納場所として決定する決定手段と、前記デジタルデータを決定手段により決定された記憶手段に格納する格納手段とを含むことを特徴とすることもできる。

【００７７】これによって、空いている記憶領域を確保できる記憶手段のうち、一番高い保護レベルが設定されている記憶手段を格納先として特定することができるので、それぞれのデジタルデータをできるだけ安全に記録することができる。また、セキュアデバイスにおいて、前記処理手段は、さらに、前記検索手段により何れの記憶手段も検索されなかった場合に利用者にデジタルデータを格納できない旨を提示するためのエラー情報を出力する出力手段を含むことを特徴とすることもできる。

【００７８】これによって、空いている記憶領域が無い場合に、利用者にデジタルデータを格納できない旨を提示することができる。また、セキュアデバイスにおいて、前記処理手段は、さらに、前記検索手段により何れの記憶手段も検索されなかった場合に、（１）前記入手手段により入手された格納先情報が示す第１保護レベル以上の保護レベルが設定されている記憶手段に格納されているデジタルデータのそれぞれに付加された格納先情報を読み出し、（２）読み出した格納先情報のうち、それぞれの格納先情報が示す保護レベルが、当該第１保護レベルよりも低い格納先情報を抽出し、（３）抽出した格納先情報に対応するデジタルデータを、当該第１保護レベルよりも低く、且つ、それぞれの格納先情報が示す保護レベル以上の保護レベルが設定されている記憶手段に移動することにより、前記入手手段により入手されたデジタルデータを格納するための記憶領域を確保する移動手段を含み、前記格納手段は、移動手段により確保された記憶領域に前記入手手段により入手されたデジタルデータを格納することを特徴とすることもできる。

【００７９】これによって、先に格納されているデジタルデータを格納先情報に基づいて移動して、新しいデジタルデータを格納するための記憶領域を確保することができるので、それぞれのデジタルデータを価値に応じて効率よく記録することができる。また、セキュアデバイスにおいて、記処理手段は、さらに、前記移動手段により記憶領域を確保できない場合に利用者にデジタルデータを格納できない旨を提示するためのエラー情報を出力する出力手段を含むことを特徴とすることもできる。

【００８０】これによって、先に格納されているデジタルデータを移動しても記憶領域を確保できない場合に、利用者にデジタルデータを格納できない旨を提示することができる。また、セキュアデバイスにおいて、前記複数の記憶手段にはそれぞれ保護レベルが設定されており、前記格納先情報は保護レベルを示し、さらに、前記対応するデジタルデータの格納先として当該保護レベルが設定されている記憶手段のみを格納先として特定するか、及び、当該保護レベルが設定されている記憶手段以上の保護レベルが設定された記憶手段を格納先として特定するかのどちらかを指定し、前記処理手段は、前記格納先情報に従い前記格納先情報が示す保護レベルが設定されている記憶手段を、又は、前記格納先情報が示す保護レベル以上の保護レベルが設定されている記憶手段のうちの１つを前記デジタルデータの格納先として特定することを特徴とすることもできる。

【００８１】これによって、保護レベルが一致する記憶手段を格納先として特定するか、保護レベルが同等以上の記憶手段を格納先として特定するかを、デジタルデータの管理者がデジタルデータ毎に設定することができるので、設定の柔軟性が高い。また、セキュアデバイスにおいて、前記格納先情報は前記対応するデジタルデータの格納先を当該セキュアデバイスにおいて格納する際に任意に決定してもよいか否かを指定し、前記処理手段は、前記格納先情報に従い任意に決定する記憶手段に、又は、前記格納先情報により特定される記憶手段に前記

デジタルデータを格納することを特徴とすることもできる。

【００８２】これによって、格納先を当該セキュアデバイスにおいて格納する際に任意に決定してもよいか否かを、デジタルデータの管理者がデジタルデータ毎に設定することができるので、設定の柔軟性が高い。また、セキュアデバイスにおいて、前記複数の記憶手段にはそれぞれ保護レベルが設定されており、前記格納先情報はデジタルデータを所定の保護レベル以下の記憶手段に格納する際に暗号化するか否かを指定し、前記処理手段は、デジタルデータを前記所定の保護レベル以下の記憶手段に格納する際に前記格納先情報に従い当該デジタルデータを暗号化して格納するか、又は、そのまま格納することを特徴とすることもできる。

【００８３】これによって、デジタルデータを所定の保護レベル以下の記憶手段に格納する際に暗号化するか否かを、デジタルデータの管理者がデジタルデータ毎に設定することができるので、設定の柔軟が高い。また、セキュアデバイス毎に固有の鍵を用いて暗号化して格納する場合には、フラッシュメモリのような保護レベルが低い記憶手段に格納したデジタルデータが、他のセキュアデバイスに不正にコピーされるといった攻撃を回避できる。

【００８４】つまり、他のセキュアデバイスに不正にコピーされたとしても、鍵が異なるので正しく復号することができないため、正常に利用できない。また、セキュアデバイスにおいて、前記複数の記憶手段にはそれぞれ保護レベルが設定されており、前記格納先情報はデジタルデータを所定の保護レベル以下の記憶手段に格納する際にデジタルデータに改竄検出用の情報を付加するか否かを指定し、前記処理手段は、デジタルデータを前記所定の保護レベル以下の記憶手段に格納する際に前記格納先情報に従い当該デジタルデータに改竄検出用の情報を付加して格納するか、又は、そのまま格納することを特徴とすることもできる。

【００８５】これによって、デジタルデータを所定の保護レベル以下の記憶手段に格納する際に改竄検出用の情報を付加するか否かを、デジタルデータの管理者がデジタルデータ毎に設定することができるので、設定の柔軟が高い。また、改竄検出用の情報を付加して格納する場合には、フラッシュメモリのような保護レベルが低い記憶手段に格納したデジタルデータや格納先情報が改竄されてデジタルデータが不正に用いられるといった攻撃を回避できる。

【００８６】つまり、デジタルデータや格納先情報が改竄されたとしても、認証処理を行うことにより改竄されていることが解るので、改竄されている場合にはデジタルデータの使用を禁止すればよい。また、セキュアデバイスにおいて、前記複数の記憶手段にはそれぞれ保護レベルが設定されており、前記格納先情報はデジタルデータを所定の保護レベル以下の記憶手段に格納する際にデジタルデータにデジタル署名を埋め込むか否かを指定し、前記処理手段は、デジタルデータを前記所定の保護レベル以下の記憶手段に格納する際に前記格納先情報に従い当該デジタルデータにデジタル署名を埋め込んで格納するか、又は、そのまま格納することを特徴とすることもできる。

【００８７】これによって、デジタルデータを所定の保護レベル以下の記憶手段に格納する際に、デジタル署名を施すか否かを、デジタルデータの管理者がデジタルデータ毎に設定することができるので、設定の柔軟が高い。また、デジタル署名を施して格納する場合には、フラッシュメモリのような保護レベルが低い記憶手段に格納したデジタルデータや格納先情報が改竄されてデジタルデータが不正に用いられるといった攻撃を回避できる。

【００８８】つまり、デジタルデータや格納先情報が改竄されたとしても、認証処理を行うことにより改竄されていることが解るので、改竄されている場合にはデジタルデータの使用を禁止すればよい。また、セキュアデバイスにおいて、前記複数の記憶手段にはそれぞれ保護レベルが設定されており、前記格納先情報は前記デジタルデータの優先度を示し、少なくとも１つの記憶手段にはデジタルデータが格納され、記憶手段に格納されているデジタルデータにはデジタルデータの優先度が設定され、記憶手段にはより優先度が高いデジタルデータがより保護レベルが高い記憶手段に格納されている状態でデジタルデータが格納されており、前記処理手段は、前記格納先情報により示される優先度に基づいて前記状態を維持したまま前記入手手段により入手されたデジタルデータを格納することを特徴とすることもできる。

【００８９】これによって、デジタルデータの管理者がデジタルデータ毎に優先度を設定しておき、優先度の高さに応じて格納先を特定することができるので、デジタルデータを効率よく記録することができる。また、セキュアデバイスにおいて、記憶手段に格納されているデジタルデータにはデジタルデータの優先度を示す格納先情報が付加されており、前記処理手段は、一番高い保護レベルが設定されている記憶手段から順に、（１）前記入手手段により入手されたデジタルデータを格納するための空いている記憶領域を確保できるか否かを判定し、（２）判定が否定的な場合に、判定対象の記憶手段に格納されているデジタルデータのそれぞれに付加された格納先情報を読み出し、（３）読み出した格納先情報のうち、それぞれの格納先情報が示す優先度が、前記入手手段により入手された格納先情報が示す優先度よりも低い格納先情報を抽出し、（４）抽出した格納先情報を含むデジタルデータを、移動するデジタルデータ対応する保護レベルより低い保護レベルが設定されている記憶手段に移動し、（５）前記判定が肯定的となるまで（１）～

（４）の処理を繰り返すことにより、前記入手手段により入手されたデジタルデータを格納するための記憶領域を確保する移動手段と、移動手段により確保された記憶領域に前記入手手段により入手されたデジタルデータを格納する格納手段とを含むことを特徴とすることもできる。

【００９０】これによって、先に格納されているデジタルデータを優先度に基づいて移動して、新しいデジタルデータを格納するための、できるだけ高い保護レベルが設定されている記憶領域を確保することができるので、それぞれのデジタルデータをできるだけ安全に記録することができる。また、セキュアデバイスにおいて、前記移動手段により読み出された格納先情報はデジタルデータを移動する場合に暗号化するか否かを指定し、前記移動手段は、移動すべきデジタルデータに付加された格納先情報に従い当該デジタルデータを暗号化して移動するか、又は、そのまま移動することを特徴とすることもできる。

【００９１】これによって、デジタルデータを移動する際に暗号化するか否かを、デジタルデータの管理者がデジタルデータ毎に設定することができるので、設定の柔軟が高い。また、セキュアデバイス毎に固有の鍵を用いて暗号化して移動する場合には、フラッシュメモリのような保護レベルが低い記憶手段に移動したデジタルデータが、他のセキュアデバイスに不正にコピーされるといった攻撃を回避できる。

【００９２】つまり、他のセキュアデバイスに不正にコピーされたとしても、鍵が異なるので正しく復号することができないため、正常に利用できない。また、セキュアデバイスにおいて、前記移動手段により読み出された格納先情報はデジタルデータを移動する場合にデジタルデータに改竄検出用の情報を付加するか否かを指定し、前記移動手段は、移動すべきデジタルデータに付加された格納先情報に従い当該デジタルデータに改竄検出用の情報を付加して移動するか、又は、そのまま移動することを特徴とすることもできる。

【００９３】これによって、デジタルデータを移動する際に改竄検出用の情報を付加する否かを、デジタルデータの管理者がデジタルデータ毎に設定することができるので、設定の柔軟が高い。また、改竄検出用の情報を付加して移動する場合には、フラッシュメモリのような保護レベルが低い記憶手段に移動したデジタルデータや格納先情報が改竄されてデジタルデータが不正に用いられるといった攻撃を回避できる。

【００９４】つまり、デジタルデータや格納先情報が改竄されたとしても、認証処理を行うことにより改竄されていることが解るので、改竄されている場合にはデジタルデータの使用を禁止すればよい。また、セキュアデバイスにおいて、前記移動手段により読み出された格納先情報はデジタルデータを移動する際にデジタルデータに

デジタル署名を埋め込むか否かを指定し、前記移動手段は、移動すべきデジタルデータに付加された格納先情報に従い当該デジタルデータにデジタル署名を埋め込んで移動するか、又は、そのまま移動することを特徴とすることもできる。

【００９５】これによって、デジタルデータを移動する際にデジタル署名を施すか否かを、デジタルデータの管理者がデジタルデータ毎に設定することができるので、設定の柔軟が高い。また、デジタル署名を施して移動する場合には、フラッシュメモリのような保護レベルが低い記憶手段に移動したデジタルデータや格納先情報が改竄されてデジタルデータが不正に用いられるといった攻撃を回避できる。

【００９６】つまり、デジタルデータや格納先情報が改竄されたとしても、認証処理を行うことにより改竄されていることが解るので、改竄されている場合にはデジタルデータの使用を禁止すればよい。また、セキュアデバイスにおいて、前記格納先情報は、さらに、保護レベルを示し、前記移動手段は、前記入手手段により入手された格納先情報が示す保護レベルより低い保護レベルが設定されている記憶手段においては前記処理を行わず、前記処理手段は、さらに、移動手段により記憶領域を確保できない場合に利用者にデジタルデータを格納できない旨を提示するためのエラー情報を出力する出力手段を含むことを特徴とすることもできる。

【００９７】これによって、デジタルデータの管理者が、さらに、デジタルデータ毎に保護レベルを設定しておき、保護レベルが低い記憶手段に対しては移動処理を行わないので、デジタルデータの安全性を確保することができる。また、記憶領域を確保できない場合に、利用者にデジタルデータを格納できない旨を提示することができる。

【００９８】また、セキュアデバイスにおいて、前記入手手段により入手されるデジタルデータはコンピュータプログラムであり、複数のサブプログラムを含み、サブプログラム毎に格納先情報が付加されており、前記処理手段は、サブプログラム毎にそれぞれに付加された格納先情報により特定される記憶手段に、対応するサブプログラムを格納することを特徴とすることもできる。

【００９９】これによって、デジタルデータの管理者が、サブプログラム毎に格納先情報を設定しておき、格納先情報に基づいて、サブプログラム毎に格納先の記憶手段を特定することができるので、各サブプログラムの価値に応じて効率よく記録することができる。また、セキュアデバイスにおいて、前記複数の記憶手段にはそれぞれ保護レベルが設定されており、前記入手手段により入手されるデジタルデータはコンピュータプログラムであり１つのメインルーチンと複数のサブルーチンを含み、各ルーチン毎に格納先情報が付加され特にメインルーチンに付加された格納先情報は保護レベルが高い記憶

手段に格納すべき事を示し、前記処理手段は、ルーチン毎にそれぞれに付加された格納先情報により特定される記憶手段に、対応するルーチンを格納することを特徴とすることもできる。

【０１００】これによって、デジタルデータの管理者が、ルーチン毎に格納先情報を設定しておき、格納先情報に基づいて、ルーチン毎に格納先の記憶手段を特定することができるので、各ルーチンの価値に応じて効率よく記録することができる。特に、メインルーチンを保護レベルの高い記憶素子に格納することによってプログラムを難化することができる。

【０１０１】また、セキュアデバイスにおいて、前記入手手段により入手されるデジタルデータには、当該デジタルデータに付加された格納先情報の正当性を示し、又は、当該デジタルデータと格納先情報の対応が正しいことを示すデジタル署名が埋め込まれているか、又は、認証子が付加されており、前記処理手段は、前記デジタル署名、又は、認証子に応じた認証を実施し、当該認証が成功した場合に限り前記デジタルデータを格納することを特徴とすることもできる。

【０１０２】これによって、格納先情報とデジタルデータとが切り離せないので、安全性が高い。

【図面の簡単な説明】

【図１】本発明の実施の形態１に係るセキュアシステムの構成を示す図である。

【図２】本発明の実施の形態１に係るセキュアデバイス１００の構成を示す図である。

【図３】本実施の形態１における付加情報を示す図である。

【図４】本発明の実施の形態１に係るセキュアデバイス１００における、プログラムのダウンロード処理の動作を示す図である。

【図５】本発明の実施の形態２に係るセキュアデバイス２００の構成を示す図である。

＊【図６】本実施の形態２における付加情報を示す図である。

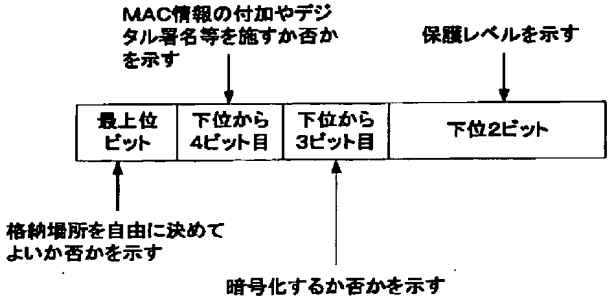
【図７】本発明の実施の形態２に係るセキュアデバイス２００における、プログラムのダウンロード処理の動作を示す図である。

【符号の説明】

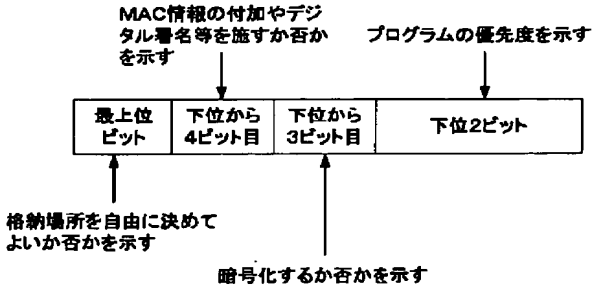
１０　セキュアデバイス
１１　カードインタフェース回路
１２　ＴＲＭ
１３　暗号処理エンジン
１４　セキュリティ鍵情報
１５　ＣＰＵ
１６　ＲＯＭ
１７　ＲＡＭ
１８　フラッシュメモリ
１９　ＥＥＰＲＯＭ
２０　付加情報処理部
１００　セキュアデバイス
１０１　プログラム入手部
１０２　低保護レベル記憶部
１１０　ＴＲＭ
１１１　付加情報解析部
１１２　領域検索部
１１３　保護レベル判定部
１１４　移動部
１１５　プログラム格納部
１１６　エラー出力部
１１７　暗号処理部
１１８　高保護レベル記憶部
２００　セキュアデバイス
２１０　ＴＲＭ
２１３　保護レベル判定部
２１４　移動部

＊

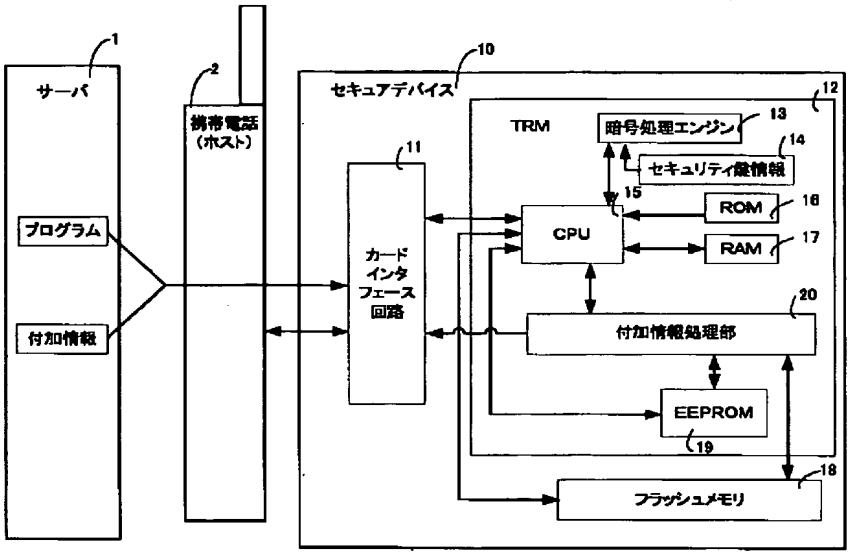
【図３】



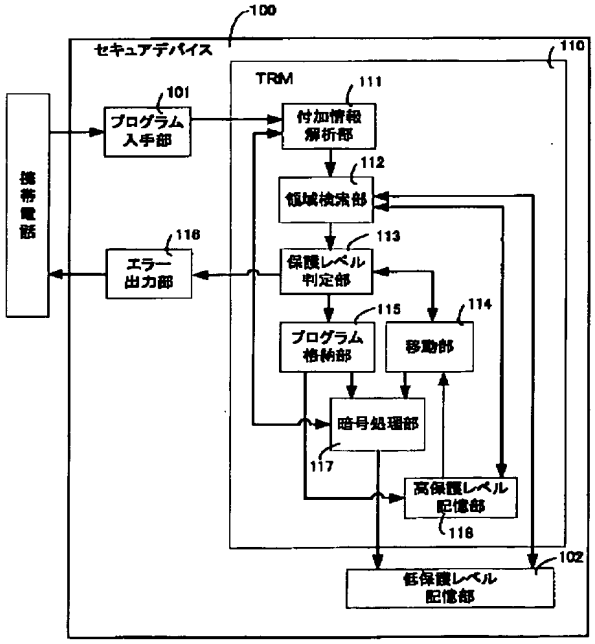
【図６】



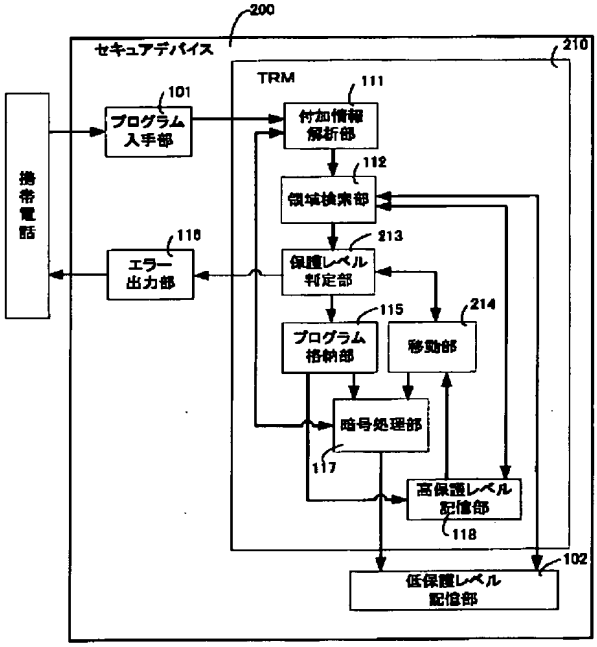
【図１】


1
サーバ
2
携帯電話
(ホスト)
10
セキュアデバイス
12
TRM
暗号処理エンジン
13
14
セキュリティ鍵情報
15
ROM
16
CPU
RAM
17
11
カード
インタ
フェース
回路
20
付加情報処理部
EEPROM
19
18
フラッシュメモリ
プログラム
付加情報

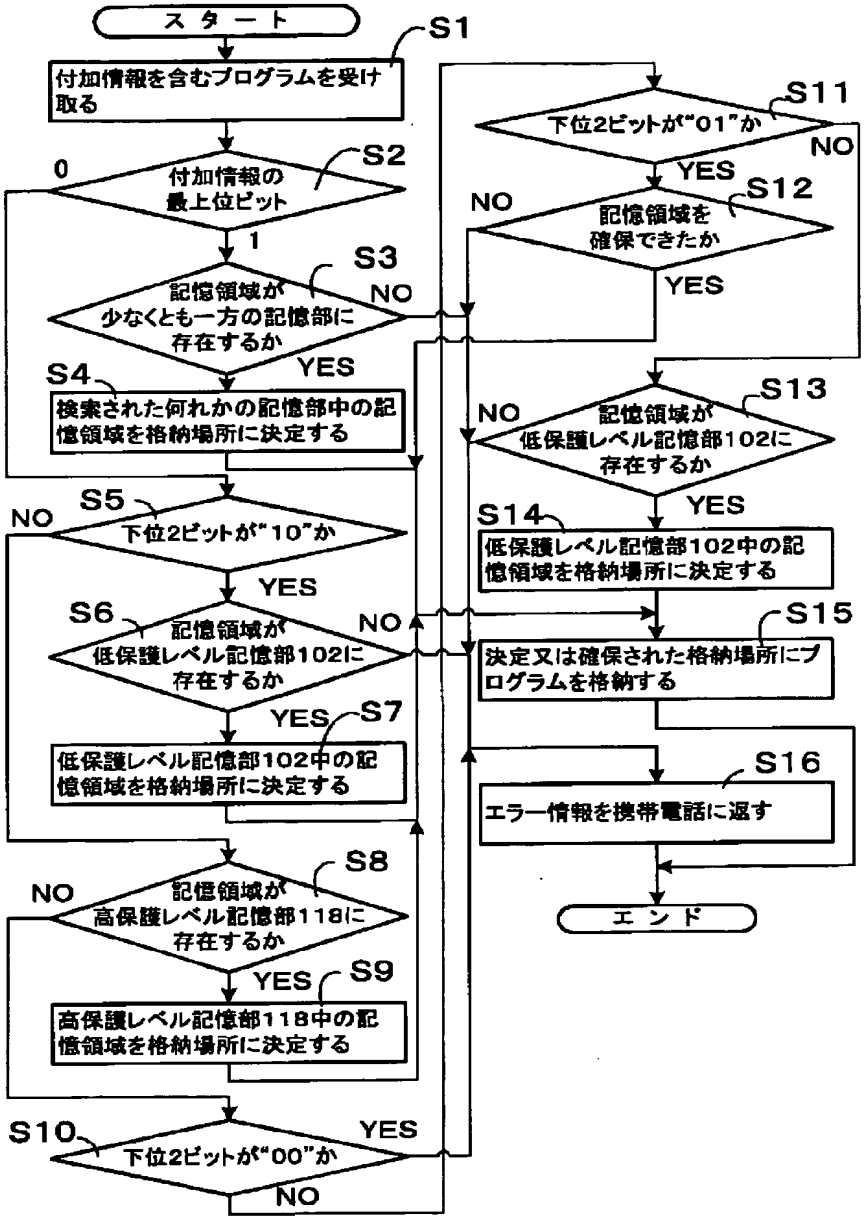
【図２】


100
セキュアデバイス
110
TRM
101
プログラム
入手部
111
付加情報
解析部
112
領域検索部
113
保護レベル
判定部
116
エラー
出力部
115
プログラム
格納部
114
移動部
暗号処理部
117
高保護レベル
記憶部
118
102
低保護レベル
記憶部
携帯電話

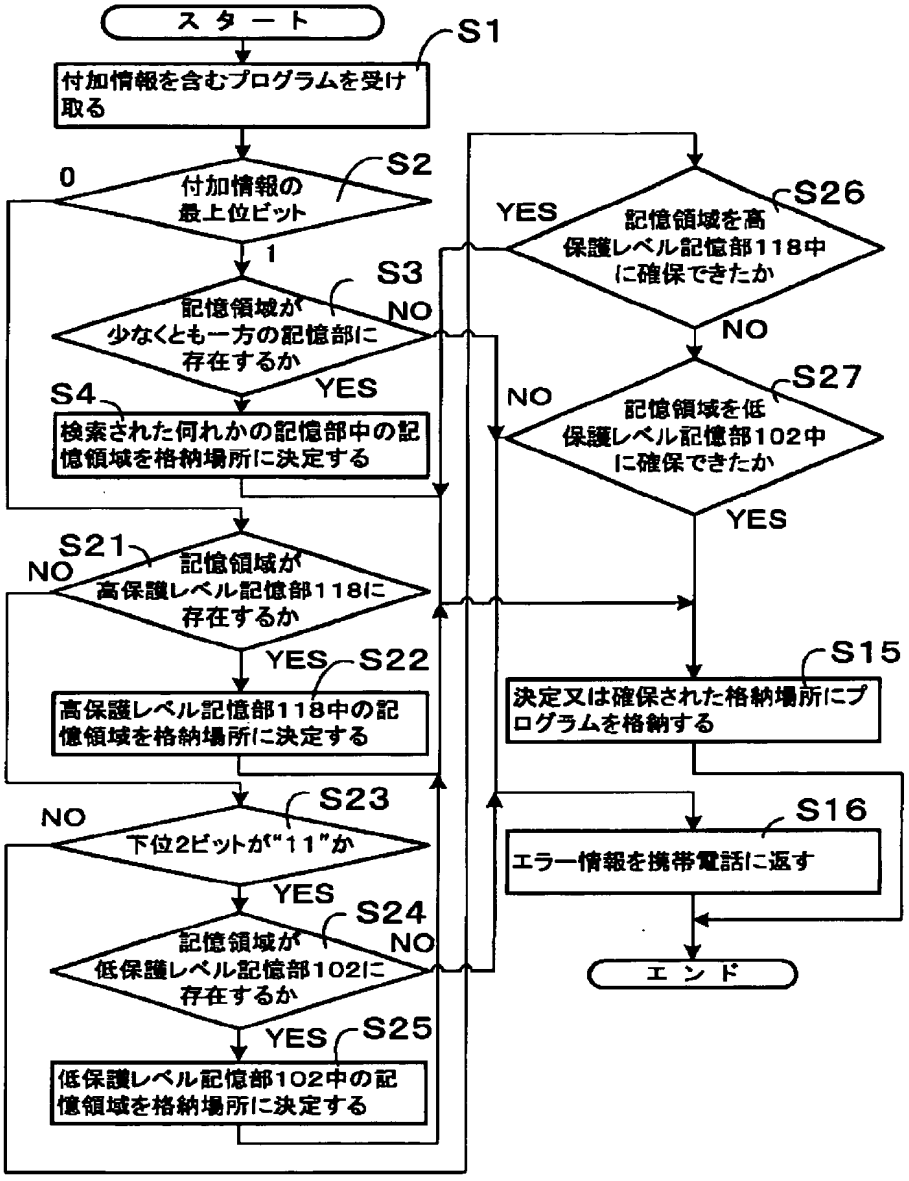
【図５】


200
セキュアデバイス
210
TRM
101
プログラム
入手部
111
付加情報
解析部
112
領域検索部
213
保護レベル
判定部
116
エラー
出力部
115
プログラム
格納部
214
移動部
暗号処理部
117
高保護レベル
記憶部
118
102
低保護レベル
記憶部
携帯電話

【図４】


スタート
S1
付加情報を含むプログラムを受け取る
S2
付加情報の最上位ビット
0
1
S3
記憶領域が少なくとも一方の記憶部に存在するか
NO
YES
S4
検索された何れかの記憶部中の記憶領域を格納場所に決定する
S5
下位2ビットが"10"か
NO
YES
S6
記憶領域が低保護レベル記憶部102に存在するか
NO
YES
S7
低保護レベル記憶部102中の記憶領域を格納場所に決定する
S8
記憶領域が高保護レベル記憶部118に存在するか
NO
YES
S9
高保護レベル記憶部118中の記憶領域を格納場所に決定する
S10
下位2ビットが"00"か
YES
NO
S11
下位2ビットが"01"か
NO
YES
S12
記憶領域を確保できたか
NO
YES
S13
記憶領域が低保護レベル記憶部102に存在するか
NO
YES
S14
低保護レベル記憶部102中の記憶領域を格納場所に決定する
S15
決定又は確保された格納場所にプログラムを格納する
S16
エラー情報を携帯電話に返す
エンド

【図７】



フロントページの続き

(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Ｆターム(参考)　5B017 AA07 CA14 CA15
5B035 AA00 BB09 CA11 CA29 CA38
5B076 BB06 FB06
5J104 AA08 AA09 AA14 AA16 DA02 PA14